AF/Ffw

TRANSMITTAL LETTER
(General - Patent Pending)

Docket No.
STS-P024-01

In Re Application Of:
Robert W. Rodenbeck et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/803,434	03/18/2004	Brown, V.	27268	2635	5439

Title:
WIRELESS SECURITY CONTROL SYSTEM

COMMISSIONER FOR PATENTS:

Transmitted herewith is:

Appeal Brief (in triplicate)

in the above identified application.

- ☐ No additional fee is required.
- ☐ A check in the amount of is attached.
- ☒ The Director is hereby authorized to charge and credit Deposit Account No. **02-0390** as described below.
  - ☐ Charge the amount of
  - ☐ Credit any overpayment.
  - ☒ Charge any additional fee required.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Ryan C Barker
Signature

Dated: 5/15/06

Ryan C. Barker
Reg. No. 47,405
BAKER & DANIELS LLP
300 N. Meridian St., Suite 2700
Indianapolis, IN 46204
(317) 237-1194
Facsimile (317) 237-1000

cc:

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

May 15, 2006
(Date)

D Cwiklinski

Signature of Person Mailing Correspondence

D. Cwiklinski

Typed or Printed Name of Person Mailing Correspondence

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of

Applicants:	Rodenbeck et. al.	)	
		)	Group Art Unit: 2635
Application No.:	10/803,434	)	Examiner: Brown, V
		)	
Filed:	March 18, 2004	)	
		)	
For:	WIRELESS SECURITY CONTROL SYSTEM	)	

APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal of the Final Official Action dated August 9, 2005 issued in respect of the above-identified application, finally rejecting claims 1-7, 10-16, and 18-29. Pending claims 1-7, 10-16, and 18-29 are provided in the attached claims appendices.

I. Real Party in Interest

The real party in interest is Stanley Security Solutions, Inc., located at 6161 East 75th St., Indianapolis, Indiana 46250.

II. Related Appeals and Interferences

There are no other appeals or interferences known to Appellant, the Appellant's legal representative, or assigns which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Allowed claims:	None
Claims objected to:	None
Claims rejected:	1-7, 10-16, and 18-29
Claims appealed:	1-7, 10-16, and 18-29

IV. Status of Amendments

An amendment after Final under 37 C.F.R. §41.33(a) and 37 C.F.R. §1.116 was filed on May 12, 2006, to correct an typographical error in claim 28. At the time of submission of this Appeal Brief, this amendment has not been entered. The pending claims are provided in an appendix hereto. Two sets of claims have been provided, the first is the status of the claims without the May 12th, 2006, amendment entered, and the second set of claims shows the status of the claims if the May 12th, 2006, amendment is entered.

V. Summary of Claimed Subject Matter

The following explanation of the subject matter defined in each of the independent claims is provided with reference to page, paragraph, and line numbers in the specification, and the drawings by reference characters as required by §41.37(c)(v). These references are made to a specific embodiment(s) disclosed in the application and do not limit the scope of the independent claims to the specific embodiment(s) and should not necessarily be considered to be exhaustive.

A. Claim 1

The subject matter defined in claim 1 relates to a wireless security control system for use in a facility having a plurality of doors. The security control system includes a central access control system, such as central access control system 20 (shown in Fig. 1) and a plurality of remote access control systems, such as remote access control system 22. The remote access control systems each being adapted to control the locking and unlocking of a respective door. [page 4, paragraph 14]

Remote access system 22 contacts the central access control system 20 at predetermined times to send information and receive information regarding updates to the user database. [pages 12-13, paragraph 40] This transmission is not in response to any users making any requests for rights to unlock any of the doors.

"Each remote access control system 22 decides independently whether a particular user 12 or token 13 is granted or denied access through the door 14 to which remote access control system 22 is coupled." [pages 10-11, paragraph 34]

B. Claim 18

The subject matter defined in claim 18 relates a security control system 10 configured to control the locking and unlocking of a plurality of doors 14 in a facility. [page 4, paragraph 14] The security control system 10 includes a central access control system 20 having a central access controller 30 and a plurality of central wireless communicators 32 electrically coupled to the central access controller 30. [page 5, paragraph 17]

The security control system 10 also includes remote access control systems 22 located remotely from the central access controller 30. [page 6, paragraph 19] Each remote access control system 22 being adapted to be mounted to a respective one of the doors 14 to control locking and unlocking of the respective door 14 and being configured to communicate information wirelessly between the central access controller 30 and a plurality of remote access controllers 62. [page 6, paragraph 20]

C. Claim 29

The subject matter of claim 29 relates to a wireless security control system 10 for use in a facility having a plurality of doors 14. [page 4, paragraph 14] The wireless security control system 10 comprises a central access control system 20 in which access information is stored, and a plurality of remote access control systems 22 each being adapted to be positioned adjacent to a respective one of the doors 14 of the facility to control the locking and unlocking of the respective door 14. [page 5, paragraph 16]

The central access control system 20 wirelessly transmits access information to the plurality of remote access control systems 22 and each of the remote access control systems 22 being configured to receive wirelessly and store at least some of the access information from the central access control system 20. [page 5, paragraph 17] "Each remote access control system 22 decides independently whether a particular user 12 or token 13 is granted or denied access through the door 14 to which remote access control system 22 is coupled." [pages 10-11, paragraph 34] The plurality of remote access control systems 22 including wireless communicators 60 that are normally powered down. [page 11, paragraph 36]

VI. Grounds of Rejection to be Reviewed on Appeal

Claims 1, 2, 4, 10-12, and 24-26 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,072,402 to Kniffin et al. (hereinafter "Kniffin") in view of U.S. Patent No. 6,161,005 to Pinzon (hereinafter "Pinzon"). Claim 3 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of Pinzon and further in view of U.S. Patent No. 5,321,963 to Goldman (hereinafter "Goldman"). Claim 5 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of Pinzon and further in view of U.S. Patent No. 5,298,883 to Pilney (hereinafter "Pilney"). Claim 6 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of Pinzon and further in view of U.S. Patent No. 6,359,547 to Denison et al. (hereinafter "Denison"). Claims 7, 13-16, and 19-23 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of U.S. Patent No. 6,177,861 to MacLellan et al. (hereinafter " MacLellan "). Claims 18 and 24-26 stand rejected under 35 U.S.C. 102(e) as being anticipated by Kniffin. Claims 27-29 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of Pilney.

VII. Argument

A. Claims 1, 2, 4, 10-12, and 24-26. Rejections under 35 U.S.C. §103- Kniffin in view of Pinzon

The rejections of claims 1, 2, 4, 10-12, and 24-26 depend on the combination of Kniffin and Pinzon. As discussed in greater detail below, Kniffin teaches away from and is incompatible with Pinzon for the combination proposed by the Final Official Action. Additionally, the Official Action fails to provide a motivation to combine the references.

i. Kniffin

Kniffin relates to a SECURE ENTRY SYSTEM WITH RADIO COMMUNICATION and discloses an entry system 10 including a lock 12 with a receiver 14 integrated therein. A user who seeks access to the lock establishes communication to a clearinghouse 18. If the clearinghouse determines, by reference to a database 24, that the user should be authorized to access an identified lock, the clearinghouse causes a radio transmission to the lock 12 to be made. When the user arrives at the door, the user must be identified in the lock. In response to identification of the authorized user at the lock, a lock microprocessor CPU 30 instructs a lock mechanism 32 to unlock. See columns 2 and 3 of Kniffin.

As described above, Kniffin fails to teach or suggest "the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors" as required by amended claim 1. Additionally, it is precisely the user communication to clearinghouse 18 requesting access that causes communication between clearinghouse 18 and lock 12.

ii. Kniffin is not silent on user interaction

The Final Official action states that Kniffin is "silent on teaching access information is transmitted to the access control system independent of independent of (sic) any user making a request to unlock the door." (p. 5, ll. 2-3, August 8, 2005 Final Office Action) However, Kniffin is not silent on user involvement with the transmission of access control information. Quite oppositely, in the Official Action's statement of motivation to combine Kniffin and Pinzon, the Action states "Kniffin et al. suggest programming the locking mechanism with the access code **when access is requested**." (p. 5, ll. 8-11, August 8, 2005 Final Office Action) (emphasis added).

Additionally, "A user who seeks access to the lock establishes communication (by a cellular telephone, by a conventional telephone, or by some other communications link 16) to a clearinghouse 18. A series of voice prompts synthesized by a computer 20 at the clearinghouse and relayed to the user over the link 16 **solicits the user to identify the lock 12 to which access is desired**." (Kniffin, Col. 2, ll. 31-37)(emphasis added). "Desirably, this authorization is valid only for a predetermined time period, such as 30 minutes (the "window" period)." (Kniffin, Col. 2, ll. 51-53).

"Thus, when a user's request to access a particular lock 12' is verified by the clearinghouse 18', an authorizing (also known as enabling) signal is sent by radio to that user's key 46. Data defining a time window is also desirably sent and limits the time period within which the key is effective. The enabling data enables the key only to access the lock requested through the clearinghouse." (Kniffin, Col. 6, ll. 2-8).

"[A] user operates the cellular telephone 52 to call the clearinghouse 54 and request access to a particular lock 56. After suitable verification (by a PIN number or the like), the clearinghouse transmits an RF signal to the identified lock and causes it to briefly make itself susceptible to being unlocked (such as for 30 seconds). Within this interval, the user must perform some manual operation (such as pushing on a door) to complete the

unlocking operation. If the manual operation is not completed within the allotted period, the lock resecures itself." (Kniffin, Col. 7, ll. 20-25).

"[T]he delivery company calls a clearinghouse 66 and identifies the sequence of deliveries the truck is to make. Each possible destination is assigned an identification number, and the desired sequence is programmed by entering (using a Touch Tone pad or the like) the numbers corresponding to the scheduled deliveries in their proper order. After suitable verification checks, the clearinghouse transmits to the targeted truck access control device 64 the authorized schedule of stops, which data is received and stored in a memory 68." (Kniffin, Col. 8, ll. 15-24).

Additionally, Kniffin claim 6 states "A method of operating a secure entry system, the system including a lock that controls access to a secure area, the system further including a key and a central station, the method comprising the steps: **establishing communication between the central station and a user remote from the central station; identifying to the central station the lock to which the user seeks access;** verifying access qualifications of the user to the central station; transmitting to the key a radio enabling signal so as to enable the key to access the lock..." (emphasis added).

Accordingly, Kniffin is not silent on user involvement, but rather explicitly requires it. Thus, Kniffin teaches away from any reference where access information is transmitted to the access control system independent of any user making a request to unlock the door. Therefore, the proposed combination with Pinzon is improper.

iii. Failure to Establish Prima Facie Obviousness

The Official Action has failed to establish a case of *prima facie* obviousness. The suggested combination of Kniffin and Pinzon will make Kniffin inoperable for its intended purpose. Additionally, the Official Action fails to provide a motivation to combine by simply stating that Kniffin and Pinzon teach opposite things and then declaring them properly combinable because of their opposite teachings. Thus, the Action has failed to establish a case of *prima facie* obviousness.

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when

combined) must teach or suggest all the claim limitations.
MPEP 2143

a. Kniffin is incompatible with Pinzon

As stated above, Kniffin is not silent on user involvement, but rather explicitly requires it. Also, Kniffin employs the user request to set the timing of the access window. Failure to have the user involvement would preclude the ability of Kniffin to set temporal restrictions on when access authorization is permitted, a key feature of Kniffin. Thus, the proposed combination would render a key feature of Kniffin unworkable.

b. The action provides no motivation to combine.

The motivation provided by the Official Action for combining Kniffin and Pinzon was "because Kniffin et al. suggest programming the locking mechanism with the access code when access is requested and Pinzon teaches pre-programming the access code into a locking unit in order to change and update the access codes." (Page 5, lines 8-11, August 8, 2005 Final Office Action). To the extent the Applicant understands the Action's stated motivation to combine Kniffin and Pinzon, the action simply states that they are combinable because Kniffin teaches transmitting access dependent on user requests, and Pinzon teaches transmitting access information independent of user requests. Thus, the Official Action's statement is that because the two references teach opposite things, that they are combinable.

Teaching opposite things alone is not a motivation to combine. Use of references teaching opposite things and combining them anyway without a motivation is the clear use of impermissible hindsight. The Action fails to discuss where a motivation or suggestion is found.

> "We have noted that evidence of a suggestion, teaching, or motivation to combine may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved... The range of sources available, however, does not diminish the requirement for actual evidence. That is, the showing must be clear and particular. Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999).

The Action fails to provide a motivation to combine. Thus, the Action has failed to establish a *prime facie* case of obviousness.

Because Kniffin is not silent on user interaction, because Kniffin is inoperable under the proposed combination, and because the Action provides no motivation to combine, reversal of the Action's rejection of claims 1, 2, 4, 10-12, and 24-26 is respectfully requested.

B. Claims 3, 5, and 6: Rejections under 35 U.S.C. §103-Kniffin in View of Pinzon further in view of other references.

Claims 3, 5, and 6 depend from claim 1 and rely upon the combination of Kniffin, Pinzon, and one other reference each. As stated above, the combination of Kniffin and Pinzon is improper. Accordingly, reversal of the Action's rejection of claims 3, 5, and 6 is respectfully requested.

i. ***Claim 3***

More specifically, the rejection of claim 3 relies on the combination of Kniffin, Pinzon, and Goldman. Claim 3 requires "the antenna is mounted to the outer portion of the housing." The Action states that mounting an antenna on an outer portion of a housing of a lock would be obvious because "[o]ne skilled in the art further recognizes that an antenna is sometimes mounted on the outer portion of a housing as evidenced by communication units such as mobile and cellular phones." (August, 9, 2005, Final Official Action, p. 8, ll. 3-5).

First, the Official Action fails to provide a motivation to combine the three cited references with the exterior mounted antenna of mobile phones. The Action states that "[o]ne skilled in the art further recognizes that an antenna is sometimes mounted on the outer portion of a housing," but fails to show why one would be motivated to apply an external mounted antenna to the proposed references. Thus, the Official Action fails to provide a *prima facie* case of obviousness.

Second, mobile and cellular phones are not security devices, locks, or the like. Accordingly, mobile and cellular phones are not primarily concerned with restricting physical access and repelling unauthorized physical access to locations. Placing any piece of an access device in an external position makes the so-placed-piece in a location more vulnerable to those who would attempt to circumvent the access restricting function of the access device. Accordingly, one skilled in the art would not be motivated to take external antennas from cellular phones, and apply those to a lock that encounters people who would attempt to dismantle and circumvent the lock. Such a combination would potentially increase the pieces exposed to individuals attempting to circumvent the lock. Thus, the proposed combination is not *prima facie* obvious.

Furthermore, the Official Action fails to address all limitations of claim 3. In addition to claim 3 requiring the antenna to be mounted on the outer portion that is mounted to an outside of the door, claim 3 requires the remote wireless communicator and remote access controller to be mounted to the inner portion of the housing that is mounted on an inside of the door. The Official Action fails to discuss any teaching of having the remote wireless communicator and remote access controller being mounted to a portion of the housing on an inside of the door, and that the remote wireless communicator and remote access controller are on an opposite side of the door from the antenna. Accordingly, the Official Action has failed to make a case of *prima facie* obviousness.

While not the only example, the Official Action's rejection of claim 3 provides the most clear evidence that impermissible hindsight has crept into the in rejection of the pending claims. On sever al occasions, the Official Action ignores the teaching of the base reference, makes combinations that defeat important features of the base reference, or provided little or no motivation for making the proposed combination. Although pending claims must be considered while undertaking examination, they should not be a roadmap for making combinations. Unfortunately, this hindsight has found its way into the rejection of claim 3 and the other §103 rejections of the Official Action.

ii. ***Claim 6***

The rejection of claim 6 relies on the combination of Kniffin, Pinzon, and Denison. Claim 6 requires "each of the remote access control systems includes a local communication port adapted to provide wired communication with a portable device." Additionally, claim 1, from which claim 6 depends, requires the wireless reception of access information. Accordingly, claim 6 requires the ability for wired communication in addition to wireless communication. The Official Action cites Kniffin for wireless communication and Denison for wired communication. The Action then states that "Denison ... teaches a remote access control system that includes a local communication port as an ***alternative*** to the wireless communication means used by Kniffin et al." (August, 9, 2005, Final Official Action, p. 9, ll. 10-12). Accordingly, even by taking the Official Action's statements as fact, rather than teaching the dual presence of wired and wireless communication, the proposed combination teaches the replacement of wireless communication with wired communication. Accordingly, the Action's proposed combination does not teach the limitation of claim 6. Accordingly, the Official Action has failed to make a case of prima facie obviousness.

C. Claims 18 and 24-26: Rejections under 35 U.S.C. §102-Kniffin.

The rejections of claims 18 and 24-26 depend on Kniffin. As discussed in greater detail below, Kniffin fails to teach every limitation, the Final Official Action fails to describe where all limitations are present in Kniffin, and the Action admits that Kniffin fails to teach a limitation of claim 18.

Claim 18 requires "a central access control system having a central access controller and a plurality of wireless communicators electrically coupled to the central access controller..." Kniffin fails to teach such a limitation. Thus, the rejection is improper.

Additionally, the Final Office Action of August 9, 2005, in rejecting claim 18 fails to discuss where Kniffin teaches "a plurality of wireless communicators electrically coupled to the central access controller." Thus, the rejection is improper.

Finally, the Final Official Action, in rejecting claims 14 and 17 states that Kniffin "is silent not explicit [sic] in teaching a plurality of central wireless communicators connected to the central controller." Thus, the Action admits that Kniffin alone is insufficient to anticipate a claim with the limitation of "a plurality of wireless communicators electrically coupled to the central access controller." For all the forgoing reasons, reversal of the Action's rejection of claim 18 and 24-26 which depend therefrom is respectfully requested.

D. Claims 7, 13-16, and 19-23: Rejections under 35 U.S.C. §103-Kniffin in View of MacLellan

Claims 7, 13-16, and 19-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Kniffin in view of MacLellan. Each of claims 7, 13-16, and 19-23 depend from either claim 1 or 18. In that claims 1 and 18 have been discussed above and shown to be in condition for allowance, claims 7, 13-16, and 19-23 are also believed to be in condition for allowance. Additionally, whereas the Official action, in rejecting claim 1, employs Pinzon for the teaching of "the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors." The rejection here of claims 7 and 13-16, which depend from claim 1, fail to include Pinzon in the rejection and fail to provide a discussion of where MacLellan teaches the limitation of "the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors" for which

Pinzon was previously relied upon. Accordingly, the Official Action has failed to make a case of prima facie obviousness.

Reversal of the rejection of claims 7, 13-16, and 19-23 is respectfully requested.

E. Claims 27-29: Rejections under 35 U.S.C. §103-Kniffin in View of Pilney.

The rejections of claims 27-29 depend on the combination of Kniffin and Pilney. Claims 27 and 28 (as amended after Final) depend from claim 1. In that claim 1 has been shown to be in condition for allowance, reversal of the rejection of claims 27 and 28 is respectfully requested. Additionally, whereas the Official action, in rejecting claim 1, employs Pinzon for the teaching of "the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors." The rejections here of claims 27-28, which depend from claim 1, fail to include Pinzon in the rejection and fail to provide a discussion of where Pilney teaches the limitation of "the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors" for which Pinzon was previously relied upon. Accordingly, the Action fails to point out each limitation of claims 27 and 28.

With respect to claim 29, as discussed in greater detail below, Kniffin teaches away from and is incompatible with Pilney for the combination proposed by the Final Official Action.

i. Kniffin

As previously discussed, in Kniffin, if the clearinghouse determines, by reference to a database 24, that the user should be authorized to access an identified lock, the clearinghouse causes a radio transmission to the lock 12 to be made. See columns 2 and 3 of Kniffin. Thus, lock 12 must be "listening" for transmissions from clearinghouse 18.

ii. Failure to Establish Prima Facie Obviousness

The Official Action has failed to establish a case of *prima facie* obviousness. The suggested combination of Kniffin and Pilney will make Kniffin inoperable for its intended purpose. Accordingly, the proposed combination lacks a reasonable expectation of success. Thus, the Action has failed to establish a case of *prima facie* obviousness.

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. MPEP 2143

iii. Kniffin is incompatible with Pilney

As stated above, locks 12 of Kniffin wait for transmissions from clearinghouse 18. The way that Kniffin is ready to receive transmissions from clearinghouse is to have the wireless communicators of lock 12 powered up. Also, Kniffin selectively grants user access upon a request for access being sent by the user to the clearinghouse 18. User requests are not predictable. If the communicators of Kniffin are to be normally powered down, there must be some manner of communicating to the lock 12 when to power up so as to receive communications from clearinghouse 18. No such manner is shown or discussed. Accordingly, providing Kniffin with normally powered down communicators would result in communications from the clearinghouse not being received by lock 12 and access being denied. Thus, the proposed combination would render Kniffin unworkable. Accordingly, the proposed combination is improper for rendering an unworkable result.

Because Kniffin is inoperable under the proposed combination the Action has failed to establish a *prime facie* case of obviousness and reversal of the Action's rejection of claims 27-29 is respectfully requested.

VIII. Conclusion

In view of the above, Applicants respectfully submit that the present application is in order for allowance and respectfully request the Honorable Board of Appeals to direct the withdrawal of the rejections of the Final Official Action and the issuance of a Notice of Allowance.

Respectfully submitted,

Ryan C. Barker
Reg. No. 47,405

Attorney for Applicants

RCB

BAKER & DANIELS LLP
300 North Meridian, Suite 2700
Indianapolis, IN 46204
Telephone: 317.237.1194

CERTIFICATION OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: MAIL STOP APPEAL BRIEF-PATENTS, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 15, 2006

D. Cwiklinski
Name of Registered Representative

Signature

May 15, 2006
Date

BDDB01 4404374v1

CLAIMS APPENDIX

Listing of Claims (without submitted amendment entered)

1. A wireless security control system for use in a facility having a plurality of doors, the wireless security control system comprising

a central access control system in which access information is stored, and

a plurality of remote access control systems each being adapted to be mounted to a respective one of the doors of the facility to control the locking and unlocking of the respective door, the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors, each of the remote access control systems being configured to receive wirelessly and store at least some of the access information from the central access control system, each of the remote access control systems being configured to control the locking and unlocking of the respective door using the access information stored therein, each of the plurality of remote access control systems making a decision whether to unlock the respective door in response to a user making an attempt to unlock the door based on the access information stored therein and without having to further communicate with the central access control system.

2. The wireless security control system of claim 1, wherein each of the remote access control systems includes an antenna, an access controller, and a receiver that is electrically coupled to the antenna and that communicates the wireless information received by the antenna to the access controller.

3. The wireless security control system of claim 2, wherein each of the remote access control systems includes a housing having inner portion to be mounted on an inside of the respective door and an outer portion to be mounted on an outside of the respective door, and the antenna is mounted to the outer portion of the housing and the remote wireless communicator and remote access controller are mounted to the inner portion of the housing.

4. The wireless security control system of claim 1, wherein each of the remote access control systems is further adapted to transmit wireless information to the central access control system.

5. The wireless security control system of claim 4, wherein each of the remote access control systems includes a switch for selectively choosing between receiving and transmitting wireless information.

6. The wireless control system of claim 1, wherein each of the remote access

control systems includes a local communication port adapted to provide wired communication with a portable device.

7. The wireless security control system of claim 1, wherein at least one of the remote access control systems periodically initiates wireless communication with the central access control system and the central access control system transmits user updates to the at least one remote access control system in response to the wireless communication periodically initiated by the at least one remote access controller.

10. The wireless security control system of claim 1, wherein each of the remote access control systems comprises a reader adapted to read user data when presented to the reader, a remote access controller electrically coupled to the reader, the remote access controller being configured to determine whether the user data is valid and being adapted to unlock the lock if the data is valid, and a remote wireless communicator electrically coupled to the remote access controller, the remote wireless communicator being adapted to communicate information wirelessly between the remote access controller and the central access control system.

11. The wireless security control system of claim 10, wherein each of the remote access control systems further comprises a battery coupled to the respective reader, the respective remote access controller, and the respective remote wireless communicator.

12. The wireless security control system of claim 10, wherein the user data is stored on tokens, each of the remote access control systems is adapted to store user history information regarding which tokens were granted access, and each of the remote access control systems is configured to transmit the user history information to the central access control system on one of an as-needed basis and a regularly-scheduled basis.

13. The wireless security control system of claim 12, wherein at least one of the remote access control systems periodically initiates a data transfer with the central access control system so that user updates are transmitted to the at least one remote access control system by the central access control system and so that user history information is transmitted to the central access control system by the at least one remote access control system.

14. The wireless security control system of claim 1, wherein the central access control system comprises a central access controller and a plurality of central wireless communicators connected to the central access controller.

15. The wireless security control system of claim 14, wherein each central wireless communicator is designated to communicate wirelessly with an associated one of the

remote access control systems.

16. The wireless security control system of claim 14, wherein each central wireless communicator communicates wirelessly with more than one of the remote access control systems.

18. A security control system configured to control the locking and unlocking of a plurality of doors in a facility, the wireless security control system comprising:

a central access control system having a central access controller and

a plurality of central wireless communicators electrically coupled to the central access controller, and

a plurality of remote access control systems located remotely from the central access controller, each remote access control system being adapted to be mounted to a respective one of the doors to control locking and unlocking of the respective door, each of the remote access control systems having a remote access controller and a remote wireless communicator electrically coupled to the remote access controller, the plurality of central wireless communicators and the plurality of remote wireless communicators being configured to communicate information wirelessly between the central access controller and the plurality of remote access controllers.

19. The security control system of claim 18, wherein the central access control system further includes a bus and the central access controller is electrically coupled to the plurality of central access communicators by the bus.

20. The security control system of claim 19, wherein the bus is controlled by a local area network protocol.

21. The security control system of claim 18, wherein the plurality of central wireless communicators communicate with the central access controller and with the plurality of remote wireless communicators using RF technology.

22. The security control system of claim 18, wherein each of the remote access control systems periodically initiates wireless communication with the central access control system and the central access control system transmits user updates to the respective remote access control system in response to the wireless communication periodically initiated by the respective remote access controller.

23. The security control system of claim 18, wherein each central wireless communicator is designated to communicate wirelessly with an associated one of the remote access control systems.

24. The security control system of claim 18, wherein each central wireless communicator communicates wirelessly with more than one of the remote access control systems.

25. The security control system of claim 18, wherein each of the remote access control systems further includes a reader electrically coupled to the remote access controller and adapted to read user data and each of the remote access control systems periodically transmits the associated user data to the central access controller.

26. The security control system of claim 18, wherein each remote access controller is configured to transmit wireless information through the associated remote wireless communicator and at least one central wireless communicator to the central access controller to provide the central access controller with user access information.

27. The wireless security control system of claim 1, wherein the plurality of remote access control systems includes a wireless communicator that receives access information from the central access control system, the wireless communicators being normally powered down.

28. The wireless security control system of claim 28, wherein the wireless communicators are powered up to initiate request updated access information from the central access control system.

29. A wireless security control system for use in a facility having a plurality of doors, the wireless security control system comprising

a central access control system in which access information is stored, and

a plurality of remote access control systems each being adapted to be positioned adjacent to a respective one of the doors of the facility to control the locking and unlocking of the respective door, the central access control system wirelessly transmitting access information to the plurality of remote access control systems, each of the remote access control systems being configured to receive wirelessly and store at least some of the access information from the central access control system, each of the remote access control systems being configured to control the locking and unlocking of the respective door using the access information stored therein, each of the plurality of remote access control systems making a decision whether to unlock the respective door in response to a user making an attempt to unlock the door based on the access information stored therein, the plurality of remote access control systems including wireless communicators that are normally powered down.

Listing of Claims (with submitted amendment entered)

1. A wireless security control system for use in a facility having a plurality of doors, the wireless security control system comprising

a central access control system in which access information is stored, and

a plurality of remote access control systems each being adapted to be mounted to a respective one of the doors of the facility to control the locking and unlocking of the respective door, the central access control system wirelessly transmitting access information to the plurality of remote access control systems independent of any users associated with the access information making any requests for rights to unlock any of the doors, each of the remote access control systems being configured to receive wirelessly and store at least some of the access information from the central access control system, each of the remote access control systems being configured to control the locking and unlocking of the respective door using the access information stored therein, each of the plurality of remote access control systems making a decision whether to unlock the respective door in response to a user making an attempt to unlock the door based on the access information stored therein and without having to further communicate with the central access control system.

2. The wireless security control system of claim 1, wherein each of the remote access control systems includes an antenna, an access controller, and a receiver that is electrically coupled to the antenna and that communicates the wireless information received by the antenna to the access controller.

3. The wireless security control system of claim 2, wherein each of the remote access control systems includes a housing having inner portion to be mounted on an inside of the respective door and an outer portion to be mounted on an outside of the respective door, and the antenna is mounted to the outer portion of the housing and the remote wireless communicator and remote access controller are mounted to the inner portion of the housing.

4. The wireless security control system of claim 1, wherein each of the remote access control systems is further adapted to transmit wireless information to the central access control system.

5. The wireless security control system of claim 4, wherein each of the remote access control systems includes a switch for selectively choosing between receiving and transmitting wireless information.

6. The wireless control system of claim 1, wherein each of the remote access control systems includes a local communication port adapted to provide wired communication with a portable device.

7. The wireless security control system of claim 1, wherein at least one of the remote access control systems periodically initiates wireless communication with the central access control system and the central access control system transmits user updates to the at least one remote access control system in response to the wireless communication periodically initiated by the at least one remote access controller.

10. The wireless security control system of claim 1, wherein each of the remote access control systems comprises a reader adapted to read user data when presented to the reader, a remote access controller electrically coupled to the reader, the remote access controller being configured to determine whether the user data is valid and being adapted to unlock the lock if the data is valid, and a remote wireless communicator electrically coupled to the remote access controller, the remote wireless communicator being adapted to communicate information wirelessly between the remote access controller and the central access control system.

11. The wireless security control system of claim 10, wherein each of the remote access control systems further comprises a battery coupled to the respective reader, the respective remote access controller, and the respective remote wireless communicator.

12. The wireless security control system of claim 10, wherein the user data is stored on tokens, each of the remote access control systems is adapted to store user history information regarding which tokens were granted access, and each of the remote access control systems is configured to transmit the user history information to the central access control system on one of an as-needed basis and a regularly-scheduled basis.

13. The wireless security control system of claim 12, wherein at least one of the remote access control systems periodically initiates a data transfer with the central access control system so that user updates are transmitted to the at least one remote access control system by the central access control system and so that user history information is transmitted to the central access control system by the at least one remote access control system.

14. The wireless security control system of claim 1, wherein the central access control system comprises a central access controller and a plurality of central wireless communicators connected to the central access controller.

15. The wireless security control system of claim 14, wherein each central wireless communicator is designated to communicate wirelessly with an associated one of the remote access control systems.

16. The wireless security control system of claim 14, wherein each central

wireless communicator communicates wirelessly with more than one of the remote access control systems.

18. A security control system configured to control the locking and unlocking of a plurality of doors in a facility, the wireless security control system comprising:

a central access control system having a central access controller and

a plurality of central wireless communicators electrically coupled to the central access controller, and

a plurality of remote access control systems located remotely from the central access controller, each remote access control system being adapted to be mounted to a respective one of the doors to control locking and unlocking of the respective door, each of the remote access control systems having a remote access controller and a remote wireless communicator electrically coupled to the remote access controller, the plurality of central wireless communicators and the plurality of remote wireless communicators being configured to communicate information wirelessly between the central access controller and the plurality of remote access controllers.

19. The security control system of claim 18, wherein the central access control system further includes a bus and the central access controller is electrically coupled to the plurality of central access communicators by the bus.

20. The security control system of claim 19, wherein the bus is controlled by a local area network protocol.

21. The security control system of claim 18, wherein the plurality of central wireless communicators communicate with the central access controller and with the plurality of remote wireless communicators using RF technology.

22. The security control system of claim 18, wherein each of the remote access control systems periodically initiates wireless communication with the central access control system and the central access control system transmits user updates to the respective remote access control system in response to the wireless communication periodically initiated by the respective remote access controller.

23. The security control system of claim 18, wherein each central wireless communicator is designated to communicate wirelessly with an associated one of the remote access control systems.

24. The security control system of claim 18, wherein each central wireless communicator communicates wirelessly with more than one of the remote access control

systems.

25. The security control system of claim 18, wherein each of the remote access control systems further includes a reader electrically coupled to the remote access controller and adapted to read user data and each of the remote access control systems periodically transmits the associated user data to the central access controller.

26. The security control system of claim 18, wherein each remote access controller is configured to transmit wireless information through the associated remote wireless communicator and at least one central wireless communicator to the central access controller to provide the central access controller with user access information.

27. The wireless security control system of claim 1, wherein the plurality of remote access control systems includes a wireless communicator that receives access information from the central access control system, the wireless communicators being normally powered down.

28. The wireless security control system of claim 27, wherein the wireless communicators are powered up to initiate request updated access information from the central access control system.

29. A wireless security control system for use in a facility having a plurality of doors, the wireless security control system comprising

a central access control system in which access information is stored, and

a plurality of remote access control systems each being adapted to be positioned adjacent to a respective one of the doors of the facility to control the locking and unlocking of the respective door, the central access control system wirelessly transmitting access information to the plurality of remote access control systems, each of the remote access control systems being configured to receive wirelessly and store at least some of the access information from the central access control system, each of the remote access control systems being configured to control the locking and unlocking of the respective door using the access information stored therein, each of the plurality of remote access control systems making a decision whether to unlock the respective door in response to a user making an attempt to unlock the door based on the access information stored therein, the plurality of remote access control systems including wireless communicators that are normally powered down.

EVIDENCE APPENDIX

Appellant is unaware of any evidence entered into the record.

RELATED PROCEEDINGS APPENDIX

Appellant is unaware of any proceeding to identify pursuant to 37 CFR §41.37(c)(1)(ii).